数字版权管理系统中的使用控制模型

张海鑫，程丽红，李顺东
（陕西师范大学 计算机科学学院，陕西 西安 710062）

摘 要：文中在分析数字版权管理系统和传统访问控制三种模型不足的基础上，针对数字版权管理系统的结构特点，结合使用控制的ABC模型，提出了一种数字版权管理系统的使用控制模型——$UCON_{onA1}$模型。并根据$UCON_{onA1}$模型的特点设计了数字版权管理系统框架，给出了系统工作的流程以及系统实现的关键技术。通过应用该模型能够对权限进行动态分发，并能在使用的整个过程中持续实现对未授权访问的控制，防范资源被随意拷贝、再次分发给其他用户，保证了数字内容的合法使用。

关键词：数字版权管理；使用控制；权限
中图分类号：TP309 **文献标识码**：A **文章编号**：1673-629X(2009)12-0135-04

Usage Control Model for Digital Right Management

ZHANG Hai-xin, CHENG Li-hong, LI Shun-dong
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: According to the architecture characteristics of digital rights management system, a digital rights management usage control model - $UCON_{onA1}$, combined with the ABC model of control, was put forword through analyzing the lack of digital rights management system and three types of traditional access control model. A framework of digital rights management system was designed based on the characteristics of model - $UCON_{onA1}$. In addition, the system processes and key technologies for system were given. Application of this model could distribute the permissions dynamically. The continual control of unauthorized access could prevent resources from being copied, re-distributed to other users, which could guarantee the legitimate use of digital content.

Key words: digital right management; usage control; rights

1 概 述

1.1 数字版权管理系统介绍

数字版权管理[1]（Digital Rights Management，DRM）是指采用包括信息安全技术手段在内的系统解决方案，在保证合法的、具有权限的用户对数字媒体内容（如数字图像、音频、视频等）正常使用的同时，保护数字媒体创作者和拥有者的版权，并根据版权信息获得合法收益，而且在版权受到侵害时能够鉴别数字信息的版权归属及版权信息的真伪。数字版权保护不是密码技术的简单应用，也不是将受保护的内容从服务器传递到客户端并用某种方式限制其使用的简单机制。内容提供者希望通过使用DRM，保护数字作品的版权，促进数字化市场的发展。

收稿日期：2009-04-10；**修回日期**：2009-07-26
基金项目：国家自然科学基金（60673065）
作者简介：张海鑫（1985-），男，甘肃张掖人，硕士研究生，研究方向为网络与信息安全；李顺东，教授，博士生导师，研究方向为多方保密计算、密码学与信息安全。

DRM系统对数字信息的保护控制需要实施集中管理和分散控制相结合的保护控制机制。保护控制机制的实施需要可信服务器和可信客户机的协调完成（服务器和客户机双方是相互信任的）。它具有以下一些基本的保护控制的需求[2]：

（1）对数字内容的持久保护。对数字内容在系统中生命周期的全过程的使用状况实施保护和控制；

（2）数字权利的管理。包括权利的颁发、交易、代理和回收；

（3）对用户私有信息的保护（这一点被大多数DRM系统所忽略）。由于DRM需要由客户端向服务器客户端提供用户的私有信息以向用户颁发许可，用户的私有信息可能被服务商故意泄露。而且由于在DRM系统中需要跟踪受保护的数字内容的使用、传播和交易等使用过程，这就可能会泄露用户之间的组织信息。

1.2 传统访问控制

数字版权管理中一个重要的方面是对数字资源的使用进行可靠控制。访问控制是通过某种途径显式地

允许或限制主体对客体访问能力及范围的一种方法。它是针对越权使用系统资源的防御措施，访问控制的目的在于限制系统内用户的行为和操作，包括用户能做什么和系统程序根据用户的行为应该做什么两个方面。

传统访问控制[3]的 3 种主要策略有：自主访问控制(DAC)、强制访问控制(MAC)和基于角色的访问控制(RBAC)，它们目前已经被广泛应用于包括 DRM 在内的各种领域。

但是随着网络的发展和广泛应用，网络上以数字形式广泛传播着大量数字作品。用传统访问控制策略保护数字版权存在下面的问题：

(1)权限是静态的。在执行任务之前，主体就拥有权限，不考虑操作的上下文，不适合于动态的异构的分布式系统。并且，主体一旦拥有某种权限，在任务执行过程中或任务执行完后，会继续拥有这种权限。然而，在许多应用中，权限需要根据主体的行为而修改。例如，一个主体被授权观看数字作品一次，在主体执行一次观看操作后，权限应当变为“禁止观看”。这种权限的可变性在传统的访问控制中很少被讨论。

(2)传统访问控制只能在执行任务之前授权。但是现代访问控制要求在数字作品创建、传播和使用整个过程中持续实现对未授权访问的控制、防范资源被随意拷贝、再次转发给其他用户等。

(3)传统访问控制侧重于对封闭环境中数字作品的保护，通过在服务器端设置参考监视器实现对服务器中数字资源的访问控制。一旦数字信息被访问过或传播到其它系统后，它就不能保护这些数字信息。

(4)传统的访问控制仅仅处理已知用户的访问，控制的实现主要基于已知用户的身份和属性，这显然不适合于今天的 Internet 世界。因为今天的网络是一种高度动态的和分布的计算环境，数字信息很可能被匿名用户使用，也可能存储在不同的地方，因此需要不管用户位置还是信息位置，都能得到保护。

对于上述访问控制问题，尽管其中的某些问题已经在一些访问控制文献中讨论过，但它们通常限定在某些特定的问题上，因此其讨论并不是全面的。文中使用控制模型将多个因素集成到统一的框架中来克服传统的访问控制模型的不足，对传统的访问控制进行了扩充。

2 使用控制模型

2002 年，George Mason 大学著名的信息安全专家 Ravi Sandhu 教授和 Jaehong Park 博士首次提出使用控制[4](UCON，Usage Control)。

2.1 使用控制的 ABC 模型

UCON 模型又称为 ABC 模型，主要目标是保护数据资源，防止非安全操作的发生。连续性和可变性是它的两个新特征。ABC 模型由如下 8 个部分组成：主体、主体属性、客体、客体属性、权限、授权、义务和条件(参见图 1)。

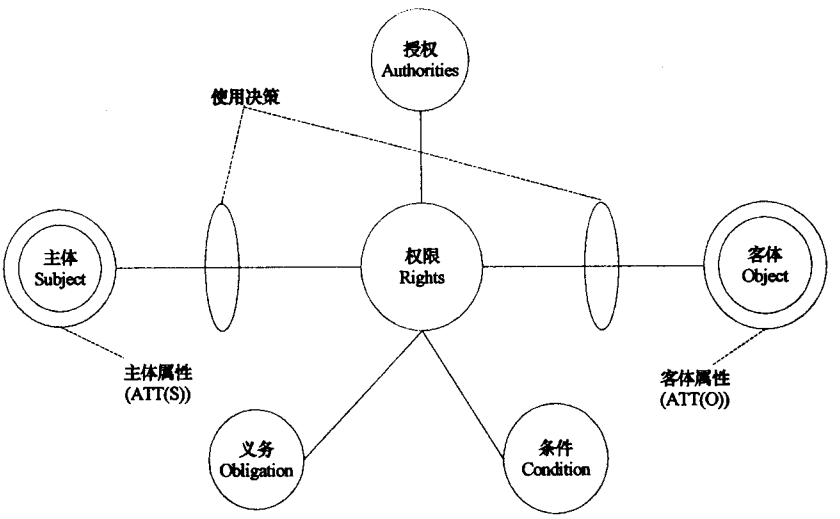

图 1 ABC 模型

主体、主体属性、客体和客体属性的概念都来自于传统的访问控制模型，是较为熟悉的概念，以相似的方式应用于 UCON 模型中。权限指一个主体以特定的方式(如读或写)访问某个客体的权利。从这个意义上讲，UCON 模型的权限概念在本质上与传统访问控制模型的概念相似。它们之间微妙的区别是：UCON 模型中不再把权限看成独立于主体活动的访问控制矩阵的静态元素，而只是在主体试图访问客体时才根据主客体属性和授权、义务、条件三大决策因素动态地确定用户的操作权限。图 1 所示的使用决策函数在请求使用资源的时刻作出这个授权决定，该决定依赖于主体属性、客体属性、授权、义务和条件。

授权(A)是传统访问控制模型中唯一的权限决策因素，也是 UCON 模型中重要组成部分。授权是基于主、客体的属性和所请求的权限(如读或写权限)并依据权限规则集进行的权限判断操作。此外，执行授权谓词可能会引起主、客体可变属性值的修改，进而将对本次或其他的访问决策产生影响。例如，用户在购买一本电子图书后其信用卡上的金额会相应减少，这一结果将是用户本次或以后使用该卡进行电子交易的权限判断的重要依据。

义务(O)是强制要求主体必须在访问之前或访问过程中执行的功能性谓词。义务谓词可以在访问之前执行(preB)也可以在访问过程(onB)中执行,preB 谓词利用一些历史记录功能检查特定的行为是否已经完成,并返回"真"或"假"。属性可以用来判断使用请求需要承担哪种义务。义务有时可能需要更新主体属性。注意,属性不用来判定义务,仅用来选择申请何种义务。

条件(C)是环境的或面向系统的决策因素。条件评估当前环境或系统的状态,检查是否满足了相应请求,并返回"真"或"假"。主体属性或客体属性可以用来判断用户请求需要满足何种条件。但条件的评估并不改变任何主体或客体的属性,这一点与授权和义务不同,因为条件不受主体的直接控制。例如,用户必须在规定的终端、规定的时间段使用服务,也可以对网络流量进行一定的限制等。

2.2 ABC 的核心模型

基于授权、义务和条件 3 个因素,并结合连续性和可变属性,可以设计一套使用控制的核心模型。之所以称之为核心模型,是因为它主要集中在使用资源的实施过程中,而不包括管理方面的问题。而且,它们应用于特定的系统时需要进一步细化。

假设 ABC 模型有一个访问客体资源的请求,请求的权限可在行使该权限之前进行判断,也可在行使该权限过程中判断(连续性属性)。但却不能在权限行使之后判断,因为这对访问控制没有任何意义。可变性属性作为使用资源的结果,允许更新主体或客体的属性。如果在访问控制过程中不存在可变属性,则使用决策过程不可改变属性,用 0 表示,存在可变属性的访问控制模型中,属性的更新可能在权限行使之前、行使过程中或权限使用之后,分别用 1,2 和 3 表示。根据这些标准,有 16 种可能的模式[5]作为使用控制模型的核心模式,见表 1 所示。

表 1　16 种基本 ABC 模型矩阵

	0(不可改变)	1(使用前更新)	2(使用中更新)	3(使用后更新)
preA	Y	Y	N	Y
onA	Y	Y	Y	Y
preB	Y	Y	N	Y
onB	Y	Y	Y	Y
preC	Y	N	N	N
onC	Y	N	N	N

表 1 显示了基于授权、义务、条件 3 个决策因素和可变性、连续性两种属性的所有可能模式的细节。例如 $UCON_{preA1}$ 表示授权作为访问控制决策因素,并且在权限使用之前修改主客体有关可变属性。表 1 中对于不可能实现的情况用"N"表示,例如在以条件为单纯的决策因素的访问模型中所有更新属性的组合都标记为"N",因为条件评估不可能改变任何主客体属性。此外,在权限使用前,不可能出现使用过程中更新主客体属性的操作,所以在相应的栏目中标记"N"。

在实际系统中可能根据不同应用的需求产生不同的组合权限模型,例如 $UCON_{preCOonCO}$ 就表示既要在访问使用前执行"条件"决策因素检查又要在访问过程中检查,并且都不改变主客体的任何属性。

2.3 $UCON_{onA1}$ 模型

定义 $UCON_{onA1}$ 模型[6]具有以下成分:

(1)S,O,R,ATT(S),ATT(O)和 onA 是模型的主要组成成分,其含义分别是主体,客体,主体属性,客体属性和访问过程中授权;

(2)onA(ATT(S),ATT(O),r)表示访问过程中的权限判断谓词,表示依据 ATT(S),ATT(O),r 来判断正在执行的访问操作是否继续满足权限判断规则;

(3)在访问过程中执行预先更新操作:preUpdate(ATT(S)),preUpdate(ATT(O));

(4)allowed(S,O,r) = > true;

(5)stopped(S,O,r) < =¬ onA(ATT(S), ATT(O),r)。

如果没有预先授权,请求访问也是允许的。然而,授权检测在权限的使用过程中是激活的,onA 判断谓词在使用过程中不断进行检测。一旦主、客体属性不再满足系统的权限要求则立即执行 stopped(S,O,r),停止主体 S 对客体 O 的 r 操作。从技术实现上讲,这些检测是基于时间或基于事件的。

2.4 $UCON_{onA1}$ 模型的应用

DRM 一般使用基于支付的安全策略,这些在传统的访问控制策略中没有涉及。因此使用 $UCON_{onA1}$ 模型来实现一个简单的支付的 DRM[7]:

定义:M 为一组款数集合;

credit: S- >M 标记用户的账户上的余额;

value: O * R- >M 标记某一客体资源的消费价格;

ATT(S): {credit} 用户账户余额为主体属性;

ATT(O,r): {value} 消费价格为客体属性,这里消费价格与权限 R 有关;如:读客体资源与拷贝发布客体资源的价格是不同的。

在访问过程中,首先执行 preUpdate(ATT(S)),preUpdate(ATT(O)) 也即预先更新主体属性(用户账户余额)和客体属性(客体资源的消费价格);

allowed(S,O,r) = > credit(S)≥value(O,r),当用户账户余额不小于当前访问客体资源所需价格时,允许访问进行,否则终止访问。

3 $UCON_{onA1}$模型下 DRM 系统设计

3.1 系统框架

根据 $UCON_{onA1}$模型，设计了 DRM 系统框架[8]，如图 2 所示。该系统框架主要有内容数据库、安全容器、作品服务器、许可证管理器、电子交易系统、媒体播放器和服务器端参考监视器(SRM)等部件。其中参考监视器是执行使用控制的关键问题之一。使用控制的参考监视器[9]由使用决策设施(UDF)和使用执行设施(UEF)组成。UDF 包括授权模块、条件模块和义务模块。授权模块利用主体和客体的信息(属性)和使用规则检查请求是否被允许，它可能返回“yes”或者“no”，它也可能返回请求的对象被授权部分的元数据和允许的权力。这些元数据随后被 UEF 的定制模块用于请求数字权力。条件模块决定授权的请求是否满足条件需求(如当前时间、IP 地址等)，它可能限制提供的设备(如 CPU 的 ID 号、IP 地址)，时间(如工作时间、值班时间)等。义务模块决定是否履行一定的义务，在请求使用之前，或者在请求使用的过程中履行义务。

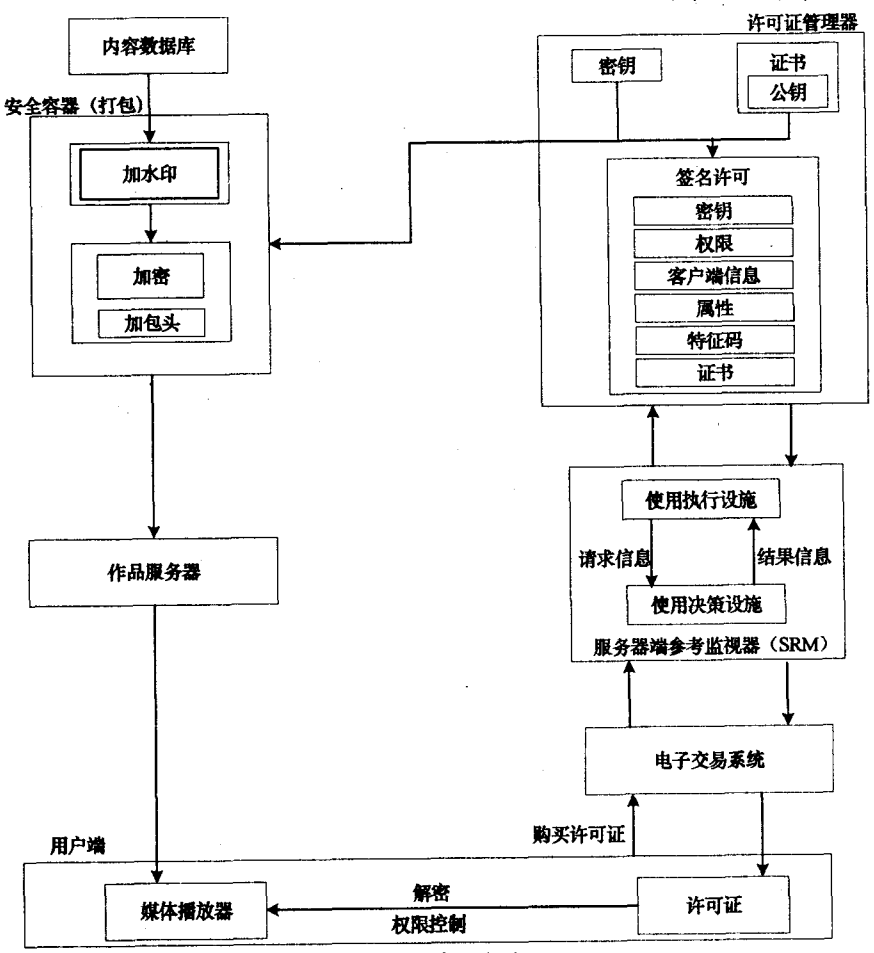

图 2 DRM 系统框架

参考监视器可设置在服务器端(称服务器端参考监视器(SRM))，也可设置在客户端(称客户器端参考监视器(CRM))。在图 2 所示的 DRM 系统框架中，将参考监视器设置在服务器端。当然服务器端参考监视器和客户器端参考监视器能在一个系统中共存。

3.2 系统的工作流程

根据图 2 所示的系统框架，$UCON_{onA1}$模型下 DRM 系统的工作流程[10]如下：

(1)用户从客户端访问作品服务器，查询内容情况，确定自身需要的内容；

(2)用户从客户端向许可证管理器发出请求，提出所需要的内容并申请所需的使用授权；

(3)许可证管理器请求作品服务器核查用户请求的内容是否可用；

(4)许可证管理器检证用户身份，例如将用户的权限请求与用户权限数据库核对；

(5)作品服务器将用户需要的内容从内容数据库取出，并控制安全容器进行打包，发送到用户的媒体播放器；

(6)服务器端参考监视器(SRM)预先更新 ATT(S)、ATT(O)，然后依据 ATT(S)、ATT(O)、r 来判断正在执行的访问操作；

(7)若 onA(ATT(S), ATT(O), r)为 true，则 allowed(S, O, r)，授予其权限，并与电子交易系统完成转账、支付等必要的财务过程；若 onA(ATT(S), ATT(O), r)为 false，则 stopped(S, O, r)，不授予其权限，终止交易。

(8)许可证管理器生成许可证，通过服务器端参考监视器(SRM)发送到电子交易系统；

(9)电子交易系统将许可证发给用户；

(10)用户端解密授权代码和数字作品，播放工具解码，显示数字内容。

在整个系统工作流程中，服务器端参考监视器(SRM)的使用执行设施不断监视并更新使用请求，防范因主客体属性的改变而使资源被滥用。

3.3 系统实现的关键技术

实现 $UCON_{onA1}$模型下 DRM 系统还需要一些关键技术，例如数字对象标识(Digital Object Identifier, DOI)、数字水

(下转第 157 页)

复位信号用作整个设计的异步复位信号。

3　1553B IP 的验证分析

为了验证 1553B IP 的功能和性能是否满足协议需求,专门开发了基于 AMBA 总线的 1553B IP 接口[5],将其互联到 AHB 总线上,搭建成基于 ARM 处理器的 SoC 验证平台,对其进行仿真验证和 FPGA 验证[6]。

在仿真验证平台上,对 1553B IP 进行了基于事务的验证[7](包括协议中规定的各种消息格式和方式命令的执行,以及异常情况的检测处理等);在 FPGA 验证平台上,对 1553B IP 进行了 RT 有效性测试(包括协议测试、电气性能测试、噪声抑制测试等)和系统应用验证。验证结果表明,在 BC 和 RT 两种方式下,1553B IP 都满足 MIL-STD-1553B 协议的要求。

4　结束语

重点论述了高速 1553B IP 的性能指标、功能结构,以及各模块的设计与实现,详细描述了高速 1553B IP 设计中应该注意的问题。其中多时钟域和异步复位的处理对其它类似设计也有一定的参考价值。

目前,高速 1553B IP 已经在 1553B 总线接口 SoC 中成功应用,并且一次性流片成功。通过 SoC 芯片的性能测试和系统验证表明,1553B IP 完全符合 MIL-STD-1553B 协议,支持 10Mbps 的高速通信。

参考文献:

[1] MIL-STD-1553B-1989 飞机内部时分制指令/响应式多路传输数据总线[S].1989.

[2] GJB 5186.1-2003 数字式时分制指令/响应式多路传输数据总线测试方法[S].2003.

[3] Clifford E. Synthesis and Scripting Techniques for Designing Multi-Asynchronous Clock Designs Rev 1.1[M]. SNUG. San Jose:[s.n.],2001.

[4] Clifford E, Mills D, Golson S. Asynchronous & Synchronous Reset Design Techniques - Part Deux Rev 1.3[M]. SNUG. Boston:[s.n.],2003.

[5] 齐利芳,贺占庄. SOPC 设计中的两种片上总线分析[J].计算机技术与发展,2006,16(1):179-181.

[6] 郭　蒙,田　泽,蔡叶芳,等. 1553B 总线接口 SoC 验证平台的实现[J].航空计算技术,2008,38(6):99-101.

[7] 韩　霞,杨洪斌,吴　悦. 面向 SoC 的事务级验证研究[J].计算机技术与发展,2007,17(3):33-36.

(上接第 138 页)

印(Digital Watermark)、数字签名(Digital Signature)、安全容器以及服务器和客户机协作时所应用的网络安全协议等。系统中一个关键的组件是许可,它代表了服务器对用户的授权。服务器必须对许可进行签名加密,以保证其信息的有效性和机密性。对许可的具体描述应基于权限描述语言[11](Rights Expression Language,REL),例如开放数字权限语言(Open Digital Rights Language,ODRL),可扩展权限描述语言(eXtensible Rights Markup Language,XrML)等。它们是 DRM 系统功能的一部分,并不是文中所讨论的使用控制模型所要特别关注的问题。

4　结束语

应用 $UCON_{onA1}$ 模型能够对权限进行动态分发,并能在使用整个过程中持续实现对未授权访问的控制、防范资源被随意拷贝、再次转发给其他用户等。为数字内容的使用提供一种更加细致和可靠的控制,保证数字内容在整个生命周期内的合法使用。

参考文献:

[1] 范科峰,莫　玮,曹　山. 数字版权管理技术及应用研究进展[J].电子学报,2007,35(6):1139-1147.

[2] 吕远大,刘文清,周雁舟. 数字版权管理系统中的角色访问控制模型[J].计算机工程,2006,32(11):180-183.

[3] 张　茹,杨　榆,张　啸. 数字版权管理[M].北京:北京邮电大学出版社,2008.

[4] Park J, Sandhu R. The UCONABC Usage Control Model[J]. ACM Transactions on Information and System Security, 2004,7(1):128-174.

[5] Zhang Xinwen, Sandhu R. Formal model and policy specification of usage control[J]. ACM Transactions on Information and System Security,2005,8(4):351-387.

[6] 彭凌西,杨　频,彭银桥,等. 使用控制访问模型的研究[J].计算机应用研究,2007,24(9):121-125.

[7] 田光辉. 使用控制理论及应用研究[D].西安:西北大学,2008.

[8] 李　丹,金　庆,吴国新. 基于 DRM 的版权管理系统的研究与设计[J].计算机技术与发展,2008,18(3):188-191.

[9] 袁　磊. 使用控制模型的研究[J].计算机工程,2005,31(12):146-148.

[10] Camp L J. First Principles of Copyright for DRM Design[J]. IEEE Internet Computing,2003,7(3):59-65.

[11] 李慧颖,赵　军,翟玉庆,等. 数字权限表达语言综述[J].计算机科学,2004,31(7):12-15.